IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

EVELINE MCCOMBS, individually, and on behalf of all others similarly situated,

Plaintiff,

v. **Case No. 22-cv-00662 JFR/KK**

DELTA GROUP ELECTRONICS, INC.

Defendant.

DEFENDANT DELTA GROUP ELECTRONICS INC.'S MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED COMPLAINT AND MEMORANDUM BRIEF IN SUPPORT

Defendant Delta Group Electronics, Inc. ("Delta"), pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), moves this Court to dismiss Plaintiff Eveline McCombs' ("Plaintiff") First Amended Complaint ("FAC") (Doc. No. 13). Pursuant to Local Rule 7.1(a), Delta conferred with Plaintiff and understands that Plaintiff intends to oppose this motion. As discussed more fully below, Plaintiff's FAC should be dismissed because:

1. Plaintiff fails to establish Article III standing because she fails to allege sufficient facts to show an injury-in-fact that is actual and imminent or fairly traceable to Delta.
2. Plaintiff fails to state a claim for negligence because there are no plausible allegations of damages, and even if there were, Plaintiff failed to allege causation.
3. Plaintiff fails to state a claim for breach of implied contract because her allegations are insufficient to establish a contractual relationship between her and Delta or to establish non-speculative damages to support the claim.
4. Plaintiff fails to state a claim for unjust enrichment because she fails to plead facts sufficient to show any benefit or that Delta has unjustly retained one.

For these and the reasons discussed below, the FAC should be dismissed with prejudice.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION.

Plaintiff Eveline McCombs ("Plaintiff") brings this putative class action for injuries she claims to have incurred as a result of an unauthorized actor's access of Delta Group Electronic, Inc.'s ("Delta") computer systems. Plaintiff alleges that she was an employee of Delta between 2019 and 2022, and that as a condition of employment she provided Delta with personal information, which was among those affected by the incident. First Amended Complaint, ECF No. 13 ("FAC") ¶ 14. Plaintiff pleads a range of generalized future injuries, including risk of future identity theft and the fear that her data "may" be exposed on the dark web. *Id.* at ¶ 45. Plaintiff also vaguely alleges that, at some unknown period of time following the incident, she experienced unauthorized attempts to access her bank account and an increase in "spam" communications, without specifying how such incidents are even remotely related to the incident. *Id.* at ¶ 98, 100. None of these allegations are sufficient to confer standing. Nor do they adequately state any claims against Delta.

Plaintiff lacks standing because she has failed to allege any sufficiently concrete injuries that are fairly traceable to Delta. Courts have consistently dismissed data breach cases where, as here, there have been only vague and conclusory allegations of misuse, future risk of injury is neither imminent nor certainly impending, and the alleged injuries cannot be fairly traced to the defendant. Indeed, Plaintiff's own admission that the fraudulent activity "may not come to light for years" demonstrates the speculative nature of her purported injuries. *Id.* ¶ 63. Even where Plaintiff offers some vague facts to suggest a misuse of her data, such allegations are entirely conclusory and devoid of any nexus between the misuse and the security incident at issue.

Even if standing can be established, all of Plaintiff's claims fail and should be dismissed under Rule 12(b)(6). Plaintiff fails to allege any plausible damages that were caused by Delta to sustain her negligence claim. Plaintiff's alleged injuries for lost time, future risk of fraud, diminution of value of her data, and potential future costs are nominal and speculative—and any allegations of emotional distress damages are unrecoverable.

Plaintiff also fails to state a claim for breach of implied contract. Courts have frequently dismissed breach of implied contract claims where the employee, like Plaintiff, fails to allege any specific policies, manuals, or assurances by the company that would manifest a contractual relationship. Plaintiff also fails to adequately allege non-speculative damages for a breach of implied contract claim.

Plaintiff's unjust enrichment claim similarly fails. Aside from conclusory references to unspecified "profits," Plaintiff does not allege exactly what benefit Delta retained such that it was unjustly enriched by an unauthorized actor accessing its computer systems. Plaintiff, as an employee, presumably received compensation in exchange for her services. Thus, it is implausible to claim that Delta was unjustly enriched.

Accordingly, the Court should dismiss the FAC under Rule 12(b)(1) for lack of standing or, alternatively, for failure to state a claim under Rule 12(b)(6).

II. PROCEDURAL HISTORY.

On September 9, 2022, Plaintiff filed her initial putative class action complaint alleging claims for negligence, breach of implied contract, and unjust enrichment. Following a meet and confer with Delta, on December 9, 2022, Plaintiff filed a First Amended Complaint ("FAC"), which, in contrast to the prior complaint, featured new allegations concerning purported attempts to access her bank account and spam communications. Notwithstanding these new allegations, the FAC should be still be dismissed for lack of standing, or alternatively, for failure to state a claim upon which relief can be granted.

III. FACTUAL ALLEGATIONS.

Plaintiff alleges that Delta is a New Mexico corporation and a "leader in Electronic Contract Manufacturing Services" with over 300 employees specializing in circuit card assembly, cable/wire harness, full system integration, and FAA repair. FAC ¶ 25-26. Plaintiff was employed by Delta from 2019 to 2022, and claims that as a condition of her employment she was required to provide Delta with personal and financial information. *Id.* ¶ 14.

Plaintiff alleges that she received a letter dated June 17, 2022, informing her that an

unauthorized third-party had gained access to certain Delta computer systems from November 2nd through November 5th, 2021. *Id.* ¶ 19. Plaintiff was informed that Delta "promptly took steps" to secure the system, engaged a cybersecurity firm to assist, and completed an investigation. *Id.* ¶ 38. After the investigation, Delta determined that some of Plaintiff's personal and financial information was involved in the data breach. *Id.* ¶ 19. Plaintiff further alleges that Delta failed to provide prompt and sufficient notice regarding the breach. *Id.* ¶ 87.

Plaintiff believes that her data "may end up for sale on the dark web" or may lead to "targeted marketing" and that she is "left to speculate" about the impact of the incident. *Id.* ¶¶ 44, 45. Plaintiff asserts that the "fraudulent activity resulting from the Data Breach may not come to light for years." *Id.* ¶ 63. Plaintiff generally alleges that she suffered anxiety, annoyance, increased risk of fraud and misuse, diminution in value of personal information, as well as lost time in verifying the impact of the incident, self-monitoring accounts, and seeking legal counsel. *Id.* ¶ 20-23.

In addition to her "generalized threat of future harm," Plaintiff also vaguely alleges that at some unknown point after the breach, she experienced unauthorized attempts to access her bank account, which she subsequently closed. *Id.* ¶ 98. Plaintiff also claims she received a "deluge" of spam calls, emails, and texts from "cybercriminal[s] trying to defraud her." *Id.* at ¶ 100. For both alleged events, which were not included in her original Complaint, Plaintiff fails to provide any details that would suggest a causal connection with or link to the Delta security incident.

IV. PLAINTIFF LACKS ARTICLE III STANDING.

Standing doctrine arises out of Article III of the U.S. Constitution's "cases" and "controversies" confinement on judicial power. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). Standing requires the plaintiff to have a sufficient "personal stake" in the case, which the Supreme Court has reduced to three elements: (1) the plaintiff suffered an injury in fact that is concrete, particularized, and actual or imminent; (2) the defendant's conduct likely caused the plaintiff's injury; and (3) the plaintiff's requested relief will likely redress the injury. *Id.* (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992)).

A party may move to dismiss a complaint for lack of standing under Federal Rule of Civil Procedure 12(b)(1) for failure to establish subject matter jurisdiction. *See Hill v. Vanderbilt Cap. Advisors, LLC*, 702 F.3d 1220, 1224 (10th Cir. 2012) ("Our court has repeatedly characterized standing as an element of subject matter jurisdiction"). At the motion to dismiss stage, a court evaluates standing based on the pleadings and accepts as true all material allegations in the complaint. *S. Utah Wilderness All. v. Palma*, 707 F.3d 1143, 1152 (10th Cir. 2013). Yet, the plaintiff bears the burden of demonstrating that they have standing. *Transunion*, 141 S. Ct. at 2207. Standing is not "dispensed in gross," therefore plaintiffs must demonstrate standing for "each claim they press and for each form of relief that they seek." *Id.* at 2208. The party seeking jurisdiction has the burden to "clearly [] allege facts" that demonstrate standing. *Schaffer v. Clinton*, 240 F.3d 878, 883 (10th Cir. 2001) (citation omitted).

A. Article III standing in data breach cases.

Standing in data breach cases presents unique issues because, for purposes of Article III standing, an injury in fact is an "invasion of a legally protected interest" that is both "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560 (internal quotation marks omitted). There must also be a "causal connection between the injury and the conduct complained of," the injury must be "fairly traceable" to the challenged action and not the result of "some third party not before the court." *Id.* A "concrete" injury means it must actually exist—it must be "real, and not abstract." *TransUnion*, 141 S. Ct. at 2204 (citing *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016) (internal quotation marks omitted)). The "threatened injury must be certainly impending to constitute injury in fact." *Clapper v. Amnesty Intern. USA*, 568 U.S. 398, 409 (2013) (emphasis removed) (quotations omitted).

Standing in data breach cases is frequently challenged, and frequently found lacking, because of the difficulty of establishing injury in fact and causation, particularly when there are only tenuous or hypothetical claims of fraud, identity theft, or misuse of data. Courts in different circuits have reached different outcomes on the issue of whether data breach victims have sustained an injury in fact depending on the particular circumstances presented and by analyzing each

claimed injury individually. *See C.C. v. Med-Data Inc.*, No. 21-2301, 2022 WL 970862, at *3-5 (D. Kan. Mar. 31, 2022) (summarizing cases in circuits finding standing as compared to cases finding no standing); *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 989-92 (W.D. Okla. 2021) (same). Although the Tenth Circuit has not addressed whether data breach victims can sustain an injury in fact merely because of a data breach, the case law among the other circuits is consistent in that standing for data breach cases still requires a concrete and imminent injury. *Compare Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (standing where laptop containing sensitive information was physically stolen and plaintiff experienced fraudulent attempt to open a new bank account using plaintiff's social security number that was on the laptop), *with Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340-44 (11th Cir. 2021) (no standing for claims of substantial future risk of identity theft, proactive mitigation costs, and conclusory allegations of unauthorized charges). Ultimately, a mere risk of something happening in the future does not satisfy the requirement that the threatened injury must be certainly impending. *See Clapper*, 568 U.S. at 410 (threatened injury must be certainly impending).

District courts in the Tenth Circuit have found a lack of standing in data breach cases with allegations similar to those here. *See, e.g.*, *Med-Data Inc.*, 2022 WL 970862, at *6, *10 (dismissing claims including future risk of identity fraud, mitigation expenses, lost time, and lost benefit of the bargain because "plaintiff's theories of standing [were] inherently speculative"); *Legg*, 574 F. Supp. 3d at 993-95 (dismissing claims of future harm, diminution of value, lost time, mitigation expenses, and annoyance); *Blood v. Labette Cnty. Med. Ctr.*, No. 22-cv-04036, 2022 WL 11745549, at *5-6 (D. Kan. Oct. 20, 2022) (dismissing claims for lack standing despite allegations of a $500 fraudulent bank account charge and issues with plaintiff's social security number when filing taxes).

B. Plaintiff has not alleged an injury-in-fact to confer standing.

Plaintiff alleges the following generalized injuries from the data breach: (1) increased risk of fraud, identity theft, and misuse; (2) diminution of value of her personal information; (3) time spent dealing with the data breach; and (4) annoyance, inconvenience, and anxiety. FAC ¶ 20-23.

Plaintiff also alleges the following "specific" injuries: attempts to access her bank account, which she subsequently closed, *id.* ¶ 98, and a purported increase in spam calls, emails, and texts since the breach, *id.* ¶ 100. None these purported injuries constitute injury in fact sufficient to constitute standing.

1. Plaintiff's alleged future harms are speculative and not imminent.

Plaintiff alleges injury from a purported increased future risk of "fraud, identity theft, and misuse." FAC ¶ 23. Plaintiff alleges that the "cybercriminals" who accessed the data had the "intent of engaging in misuse," and that personal information "may" be on the dark web. *Id.* ¶¶ 41, 45. Plaintiff also alleges that the "fraudulent activity resulting from the Data Breach may not come to light for years." *Id.* ¶ 63. Plaintiff is, thus, "left to speculate as to the full impact of the Data Breach." *Id.* ¶ 43.

The mere risk of future harm cannot, without more, qualify as a concrete harm. *See TransUnion*, 141 S. Ct. at 2211 (denying standing to some plaintiffs for lack of concrete harm based on only the "mere risk" of future harm). To confer standing, future injuries must be "certainly impending" and "allegations of possible future injury" are insufficient. *Clapper*, 568 U.S. at 409 (emphasis in original removed). Nor can Plaintiff establish standing by speculating about the "unfettered choices made by independent actors not before the court." *Lujan*, 504 U.S. at 562 (internal quotations removed); *see also Lupia v. Medicredit, Inc.*, 8 F.4th 1184, 1193 n.3 (10th Cir. 2021) (citing the recent *TransUnion* decision to "recognize the difficulties in bringing a claim for damages based on a theory of future risk of harm," in the context of standing); *Blood*, 2022 WL 11745549, at *8 (finding allegations of publication on the "dark web" insufficient, noting that "the risk of future harm is no more than an 'attenuated chain of possibilities'"). Plaintiff cannot rely on general "research and reports"—including those referenced in her FAC (*e.g.*, FAC ¶¶ 64, 67, 69-70)—about identity theft to establish a future risk of identity theft without any "particularized facts to corroborate [their] fear." *Med-Data Inc.*, 2022 WL 970862, at *7. Finally, a plaintiff cannot allege a risk of future injury when their own allegations demonstrate that the avenue for that risk has been closed. *See Engl v. Nat. Grocers by Vitamin Cottage, Inc.*, No. 15-

cv-02129, 2016 WL 8578252, at *6 (D. Colo. Sept. 21, 2016) ("Once the card was cancelled, its number, expiration date and security code were rendered useless, and consequently there is no risk … for future fraudulent purchases").

Here, Plaintiff alleges only speculative future injury, and in fact admits any injury "may not come to light for years," FAC ¶ 63, and that she is left to "speculate" about the impact of the data breach, *id*. ¶ 44. Plaintiff does not, and cannot, allege that her information was in any way published publicly, instead alleging only that her information "may end up for sale on the dark web." *Id.* ¶ 45; *cf. In re 21st Century Oncology Customer Data Sec. Breach Litig.*, 380 F. Supp. 3d 1243, 1255 (M.D. Fla. 2019) (finding adequate allegation that information has been misused to confer standing because "the third-party who accessed the Plaintiffs' personal information advertised the information for sale on the internet" and also "used the information in at least one transaction"). Moreover, Plaintiff also conveniently fails to mention that Delta has offered to provide free credit and identity monitoring services, including a $1,000,000 insurance reimbursement policy.[1] Exh. A. Regardless, Plaintiff's allegations of future risk of injury are hypothetical, speculative, and too attenuated to satisfy Article III standing requirements.

2. Plaintiff cannot manufacture standing by spending time to mitigate speculative harm.

Plaintiff alleges spending time "dealing with the consequences" of the data breach, including: "verifying the legitimacy of the data breach," "exploring credit monitoring and identity theft insurance options," "self-monitoring various accounts," and "seeking legal counsel" to mitigate the data breach. FAC ¶ 20. However, any lost time mitigating against speculative harm is

[1] Although Plaintiff repeatedly references the notice that Delta sent regarding the security incident (the "Notice"), she fails to attach it to the FAC. As provided in the Notice, Delta has provided free credit monitoring services, which include one year of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. *See* Exh. A. The Notice is properly considered on this motion and may be judicially noticed. *In re Zagg, Inc. Securities Litigation*, 797 F.3d 1194, 1201 (10th Cir. 2015)("…we are to consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12 (b)(6) motions to dismiss, in particular…matters of which a court may take judicial notice."); *S.E.C. v. Goldstone*, 952 F. Supp. 2d 1060, 1192-93 (D.N.M. 2013)(holding that consideration of facts judicially noticeable under Fed. R. Evid. 201, including facts that are a matter of public record, is proper when ruling on a motion filed under Rule 12(b)(6) and does not convert that motion into one for summary judgment under Rule 56).

insufficient for standing. A plaintiff "cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 402. The Supreme Court has explained that a plaintiff cannot "inflict[] harm on themselves" based on a hypothetical injury; if "the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure on a nonparanoid fear." *Id.* at 416. As discussed above, Plaintiff has not sufficiently alleged a risk of future harm sufficient to confer standing, and therefore, Plaintiff cannot manufacture standing by inflicting harm on herself to mitigate a risk that is not sufficiently impending.

3. Plaintiff's diminution of value claim is conclusory and speculative.

Plaintiff next alleges that personal data is a "form of intangible property" and that the value of that property has been diminished as a result of the data breach. FAC ¶ 21. Although Plaintiff discusses the value of "relevant sensitive information," she makes no concrete allegations showing how the value of her personal information has been diminished. *Id.* ¶¶ 62-71.

Courts in this circuit and others have generally found diminution of value allegations, like Plaintiff's, insufficient to confer standing without facts alleging how the plaintiff lost value. *See Legg*, 574 F. Supp. 3d at 994 ("Assuming personal identifying information has a monetary value, Plaintiff fails to allege that he attempted to sell his personal information and was forced to accept a decreased price."); *Blood*, 2022 WL 11745549, at *6 (dismissing loss of value claim because plaintiffs did not allege facts "explaining how they lost value because of the breach"); *Pruchnicki v. Envision Healthcare Corp.*, 845 F. App'x 613, 615 (9th Cir. 2021) ("Pruchnicki failed to adequately allege that *her* personal information actually lost value"). Consequently, Plaintiff's allegations concerning diminution of value are insufficient to constitute an injury in fact.

4. Plaintiff's claims of annoyance, inconvenience, and anxiety do not confer standing.

Plaintiff's claims of annoyance, inconvenience, and anxiety are insufficient for standing given the speculative risk of any harm. *See Clapper*, 568 U.S. at 416 ("[R]espondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical

future harm that is not certainly impending."); *see also Legg*, 574 F. Supp. 3d at 988, 994 (no standing where plaintiff alleged anxiety and annoyance caused by the data breach in light of speculative harm); *Krohm v. Epic Games, Inc.*, 408 F. Supp. 3d 717, 720 (E.D.N.C. 2019) ("Anxiety and anguish resulting from data breaches do not confer standing. … And without a single fact alleged to show that future harms are certainly impending, the money, time, and effort spent by plaintiff are merely self-imposed harms in response to a speculative threat.") (internal citations omitted).

5. Plaintiff's vague allegations concerning attempts to access her bank account are conclusory, and spam calls, emails, and texts, are insufficient to establish a particularized injury.

After Defendant indicated it would move to dismiss for lack of standing, Plaintiff amended her complaint to allege two incidents of purported misuse of her data. First, Plaintiff vaguely alleges that she experienced "several unauthorized attempts to access her bank account." FAC ¶ 98. Second, Plaintiff alleges that she "experienced a deluge of spam calls, emails, and texts from cybercriminal seeking to defraud her." *Id.* ¶ 100. Neither of these allegations constitute a concrete and particularized injury for purposes of standing.

Generally speaking, courts have declined to find standing where there has been no misuse of stolen information. *See Med-Data*, 2022 WL 970862, at *4 (citing cases); *see also Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1340-44 (11th Cir. 2021) ("[C]ases conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations of actual misuse or actual access to personal data.") Even where misuse of data is alleged, however, the risk of injury must still be concrete, particularized, and imminent. *See Blood*, 2022 WL 11745549, at *8-9 (allegations of data misuse insufficient to confer standing because such allegations are conclusory and speculative).

Plaintiff's allegation that she experienced unauthorized attempts to access her bank account is conclusory. FAC ¶ 98. Aside from a single sentence alleging "several unauthorized attempts" to access her bank account, plaintiff provides no other details, including: exactly when such attempts

were made, how she was put on notice, who tried to access her bank account, which bank account was accessed, whether the bank account accessed contained the same information as the financial information that was allegedly exposed, how many times the alleged attempts occurred, and any connection whatsoever between the data breach and the alleged unauthorized attempts. Without more, this allegation cannot constitute a concrete injury. And, notably, Plaintiff alleges no monetary loss.

For example, in *Blood v. Labette Cty. Med. Ctr.*, the plaintiffs alleged, *inter alia*, that they experienced "issues" with their social security numbers following a data breach when they filed their taxes in February 2022, and that they had to prove their identity before the IRS would process their tax return. 2022 WL 11745549, at *5-6. The court found that these "bare allegations are conclusory." *Id.* "The Bloods do not specify how long the delay in their tax return was, what the problem was with the return, or how difficult it was to rectify. For example, did one short phone call clear it up? And they do not even allege whether they were expecting a refund that was delayed or whether they owed taxes and had (or had not) sent their payment." *Id.*

Similarly, an alleged increase of spam calls, emails, and texts does not confer standing. In *Legg v. Leaders Life Insurance*, the court found that "the receipt of phishing emails, while perhaps 'consistent with' data misuse, does not 'plausibly suggest' that any actual misuse of Plaintiff's personal identifying information has occurred." 574 F. Supp. 3d at 993; *see also Blood*, 2022 WL 11745549, at *6 ("[T]he alleged inconvenient disruptions (such as spam calls, texts, and emails) do not constitute an injury in fact"); *In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at *5 n.8 (W.D.N.Y. 2022), *report and recommendation adopted*, 2022 WL 3045319 (W.D.N.Y. Aug. 1, 2022) (finding that, even had plaintiffs properly alleged it, an increase in spam is insufficient to constitute an injury in fact; citing a string of cases supporting the same).

In sum, none of Plaintiff's purported injuries is sufficient to satisfy Article III's requirement of an injury in fact. Accordingly, the Court should dismiss the FAC in its entirety.

C. Plaintiff's allegations concerning the attempts to access her bank account and spam calls, emails, and texts are not fairly traceable to Delta.

Even if the Court were to find that Plaintiff's allegations concerning purported attempts to access her bank account and spam calls, emails, and texts are sufficient to constitute an injury in fact, Plaintiff nonetheless fails to establish that such injuries were caused by Delta. Standing requires a "causal connection" between the injury and the conduct complained of—the injury must be fairly traceable to the defendant and not the result of "independent action of some third party not before the court." *Lujan*, 504 U.S. at 560 (internal quotation marks omitted). "[T]o show that an injury is 'fairly traceable' to the challenged conduct, a plaintiff must allege 'a substantial likelihood that the defendant's conduct caused plaintiff's injury in fact,'" which, at the motion to dismiss stage, allows for a conclusion of "but for" causation. *Santa Fe All. for Pub. Health & Safety v. City of Santa Fe, New Mexico*, 993 F.3d 802, 814 (10th Cir. 2021) (internal quotation marks omitted). A plaintiff cannot meet the burden on causation when "'[s]peculative inferences are necessary to connect [its] injury to the challenged actions.'" *Nova Health Sys. v. Gandy*, 416 F.3d 1149, 1157 (10th Cir. 2005) (citing *Simon v. E. Kentucky Welfare Rts. Org.*, 426 U.S. 26, 45 (1976)).

Plaintiff vaguely and baldly pleads that there were "attempts to access her bank account" at some unstated point. FAC ¶ 98. Other than stating that this occurred at some unspecified time *after* the data breach, Plaintiff utterly fails to allege any nexus between the two events. For example, Plaintiff does not allege that an unauthorized actor gained access to this specific bank account information through the security incident, let alone indicate any causal connection between the security incident and the unauthorized attempt, including whether information about the bank account at issue was even implicated in the breach. *See Blood*, 2022 WL 11745549, at *5 (no causation because plaintiff failed to "plead any facts suggesting how the mere possession of their Social Security numbers and names would enable someone to make unauthorized charges on an existing account (instead of, for example, opening a new account)"); *see also Smith v. Sabre Corp.*, No. 17-cv-05149, 2017 WL 11678765, at *4 (C.D. Cal. Oct. 23, 2017) (holding that plaintiff

failed to provide details of time, place, and manner of credit card charges to connect it to the data breach, and "any enterprising plaintiff could allege they experienced a fraudulent charge and attempt to connect it to any breach"); *cf. Hutton v. Nat'l Bd. of Examiners in Optometry, Inc.*, 892 F.3d 613, 623 (4th Cir. 2018) (finding plaintiffs adequately alleged causation because defendant was "the only common source" of the relevant data). Without alleging facts that indicate that Delta must exist, even to a small degree, on the causal chain leading to Plaintiff's alleged injuries, these claims are insufficient to confer standing.

Equally, Plaintiff's claimed injury of an increase in spam calls, emails, and texts fails for the simple reason that Plaintiff's phone number and email were not compromised. Delta's Notice does not mention that Plaintiff's phone number or email was involved in the breach, and Plaintiff does not allege this either. *See* Exh. A; FAC ¶¶ 18-19. In data breach cases, courts have dismissed claims on causation grounds where the information required for the alleged injury was not part of the compromised data. *See Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1086 (E.D. Cal. 2015) ("Plaintiff's allegations that … he received an increased number of email advertisements targeting his medical conditions do not allege injuries in fact fairly traceable to the Data Breach, since Plaintiff has not alleged that … email addresses were on the stolen backup data tapes."); *see also In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 33 (D.D.C. 2014) ("[Plaintiff] does not otherwise link the calls to the [stolen] tapes, claim that callers have person or private information found on the tapes, or even allege that his phone number was unlisted and hence would have been difficult for marketers to locate absent the assistance of the data thief. [Plaintiff] seems to simply be one among the many of us who are interrupted in our daily lives by unsolicited calls.").

Accordingly, even assuming that Plaintiff can establish an injury in fact from the purported "specific threats" to her data, she fails to adequately allege causation.

V. PLAINTIFF'S FAC SHOULD BE DISMISSED FOR FAILURE TO STATE ANY CLAIM UPON WHICH RELIEF CAN BE GRANTED.

Even if standing can be established, the Court should dismiss the FAC for failure to state

a claim under Rule 12(b)(6). At this stage, Plaintiff must plead "enough facts to state a claim for relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). This pleading obligation requires "more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Id.* at 555. Plaintiff must "nudge the claims across the line from conceivable or speculative to plausible" and any allegations that are "merely consistent with a defendant's liability stop short of that line." *Frey v. Town of Jackson*, 41 F.4th 1223, 1232–33 (10th Cir. 2022) (quotations omitted) (citing *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

Plaintiff's claims for negligence, breach of implied contract, and unjust enrichment should be dismissed for failure to state a claim.

A. Plaintiff's negligence claim fails for lack of plausible damages and causation.

Under New Mexico Law, "[a] negligence claim requires that the plaintiff establish four elements: (1) defendant's duty to the plaintiff, (2) breach of that duty, typically based on a reasonable standard of care, (3) injury to the plaintiff, and (4) the breach of duty as cause of the injury. *Zamora v. St. Vincent Hosp.*, 2014-NMSC-035, ¶ 22, 335 P.3d 1243 . To the extent plaintiff purports to also allege negligence per se (*see* FAC ¶¶ 93-95), injury is a required element. *See Cobb v. Gammon*, 2017-NMCA-022, ¶ 43, 389 P.3d 1058.

Plaintiff alleges that she has suffered and will suffer (1) actual identity theft; (2) the loss of opportunity of how her PII and financial information is used; (3) the compromise, publication, and/or theft of her PII and financial information; (4) out-of-pocket expenses associated with the data breach; (5) lost opportunity costs associated with attempting to mitigate the actual and future consequences; (6) continued risk to her data; (7) future costs associated with the data breach; and (8) emotional distress, loss of privacy, anxiety; (9) attempts to access her bank account; and (10) receipt of spam communications. FAC ¶¶ 95-100. These damages largely fall into three buckets: risk of future harm (e.g., risk of identity theft, loss of opportunity, continued risk, future costs), present harm (out-of-pocket expenses, time lost, loss of opportunity mitigating data breach), and emotional distress damages.

1. Plaintiff's future risk of harm is speculative and not reasonably certain.

To sustain a negligence claim, the "party seeking to recover damages has the burden of proving the existence of injuries and resulting damage with reasonable certainty." *Sanchez v. Martinez*, 1982-NMCA-168, ¶ 20, 99 N.M. 66, 653 P.2d 897; *see also First Nat. Bank in Albuquerque v. Sanchez*, 1991-NMSC-065, ¶¶ 17-18, 112 N.M. 317, 815 P.2d 613. Further, "[a]n award of damages predicated upon conjecture, guess, surmise or speculation is improper." *Martinez*, 1982-NMCA-168, ¶ 20; *see also Charlie v. Rehoboth McKinley Christian Health Care Servs.*, No. 21-cv-00652, 2022 WL 1078553, at *7 (D.N.M. Apr. 11, 2022) ("Defendant correctly points out that damages may not be awarded in New Mexico based on speculation.").

Plaintiff's allegations of future harm, *i.e.*, that she will suffer actual identity theft, future costs in mitigating future consequences of the data breach, continued risk to her data, and future risk of exposure of her data, including any future unauthorized attempts to access her bank account, are speculative and conclusory. Plaintiff has not actually suffered any actual or certain harm to date. Even if she experienced some unauthorized attempts to access her bank account, Plaintiff alleges that she closed her account and opened a new one, without suffering any actual harm beyond time spent dealing with the account. FAC. ¶ 98.

Courts have found future risk of injury too speculative to support damages for a negligence claim. In *Rehoboth*, the court found allegations concerning increased risk of harm, future out-of-pocket expenses, future time and money spent, or possible out-of-pocket costs for protective measures too speculative to support a negligence claim. *Rehoboth*, 2022 WL 1078553, at *8 (finding the same future injuries as those alleged here speculative for purposes of pleading a negligence claim); *see also Commercial Union Ins. Co. v. Lewis & Roca*, 183 Ariz. 250, 254 (Ct. App. 1995) (for a negligence action to accrue, "[t]he threat of future harm, not yet realized, is not enough," citing William L. Prosser, *Handbook on the Law of Torts* 4th ed.); *Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, *4 (C.D. Cal. June 15, 2015) ("To the extent Plaintiffs allege future harm or an increased risk in harm that has not yet occurred, those allegations do not support a claim for negligence, as they fail to allege a cognizable injury."); *see also Krottner v.*

Starbucks, 406 F. App'x 129, 131 (9th Cir. 2010) (dismissal of negligence claim despite the allegation of the "attempt to open a bank account in [plaintiff's] name" because he alleged "no loss related to the attempt") Accordingly, Plaintiff's allegations of future risk of injury are too speculative to support her negligence claim.

2. Plaintiff's purported damages for present harm, including out-of-pocket costs, lost opportunity costs in mitigating the data breach, and loss of opportunity of how her PII is used are conclusory and speculative.

Plaintiff's allegations of present harm, including out-of-pocket expenses associated with data breach, lost opportunity costs to mitigate the breach, and lost opportunity as to how her PII and financial information is used, are similarly speculative, conclusory, and insufficient. First, Plaintiff fails to identify exactly what out-of-pocket expenses she has incurred in dealing with the data breach. A vague reference to unidentified "expenses" is not enough. To the extent that it is lost time from dealing with spam calls, emails, or texts, such allegations will not support a negligence claim. *See Corona*, 2015 WL 3916744, at *4 ("[G]eneral allegations of lost time are too speculative to constitute cognizable injury."); *see also Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1322 (D. Nev. 2020), *aff'd*, 845 Fed. App'x 613 (9th Cir. 2021) ("[T]angible, out-of-pocket expenses are required in order for lost time spent monitoring credit to be cognizable as damages."); *In re Hannaford Bros. Co. Customer Data Sec. Breach Litig.*, 4 A.3d 492, 496 (Me. 2010) ("The tort of negligence does not compensate individuals for the typical annoyances or inconveniences that are a part of everyday life").

Moreover, any "lost opportunity" as to how Plaintiff's PII and financial information is used is inherently speculative. *See Razuki v. Caliber Home Loans, Inc.*, No. 17-cv-1718, 2018 WL 6018361, at *1 (S.D. Cal. Nov. 15, 2018) (finding that, for a negligence claim, "his claim alleging diminution of value of his personal data fails to allege enough facts to establish how his personal information is less valuable as a result of the breach"); *see also In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 971 (S.D. Cal. 2014) (for negligence

claim, plaintiff must show "an appreciable, non-speculative harm" when alleging diminution of value). Plaintiff's damages claims in this regard are insufficient to establish a cognizable negligence claim.

3. Plaintiff's allegations of anxiety and emotional distress are not recoverable as damages in negligence.

New Mexico does not permit recovery of damages for anxiety or emotional distress on a negligence claim. *Akutagawa v. Laflin, Pick & Heer, P.A.*, 2005-NMCA-132, ¶ 21, 138 N.M. 774, 126 P.3d 1138 ("Generally speaking, damages for emotional distress in ordinary negligence actions are not permitted in New Mexico."); *Castillo v. City of Las Vegas*, 2008-NMCA-141, ¶¶ 22-23, 145 N.M. 205, 195 P.3d 870 (emotional distress damages caused by negligent conduct permitted only in limited circumstances, for example, if the conduct also causes physical injury). Consequently, any purported anxiety or emotional distress cannot sustain Plaintiff's negligence claim.

4. Plaintiff fails to adequately allege causation resulting from the attempts to access her bank account and spam communications.

Finally, even if allegations concerning attempts to access her bank account and spam communications are sufficient to establish damages for a negligence claim, similar to the reasons for which Plaintiff cannot establish causation for standing, Plaintiff fails to adequately allege causation to establish negligence. *See Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2012) ("Generally, to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence."); *Stollenwerk v. Tri-W. Health Care All.*, 254 F. App'x 664, 668 (9th Cir. 2007) ("Of course, *purely* temporal connections are often insufficient to establish causation").

Based on the foregoing, the Court should dismiss Plaintiff's negligence claim.

B. Plaintiff does not have a plausible breach of implied contract claim.

An implied-in-fact contract is "founded upon a meeting of minds, which, although not embodied in an express contract, is inferred ... from conduct of the parties showing, in the light of

the surrounding circumstances, their tacit understanding." *Orion Tech. Res., LLC v. Los Alamos Nat. Sec.*, LLC, 2012-NMCA-097, ¶ 9, 287 P.3d 967 (internal quotation marks and citations omitted). "The existence of an implied in fact contract depends on whether the parties' representations, custom, or conduct created a reasonable expectation of contractual rights." *Armijo v. Affilion, LLC*, 854 F. App'x 236, 240 (10th Cir. 2021). "In order to state a claim for breach of an implied in fact contract, the complaint must allege facts concerning what promises were made to the plaintiff, how the promises were communicated, what the plaintiff promised in return, or how the promises created a contract." *Id.*

Aside from vague and conclusory references, Plaintiff states no facts to indicate the existence of an implied contract in which Delta promised to safeguard her information. Plaintiff alleges that she provided her personal and financial information to Delta under the "implied condition" that Delta would take reasonable measure to protect its access. FAC ¶ 17. Plaintiff then concludes that the parties "entered into implied contracts for Defendant to implement data security adequate to safeguard" Plaintiff's PII and financial information and also that Delta "solicited" Plaintiff to provide her PII as part of Delta's "regular business practices." *Id.* ¶¶ 104, 105.

However, the FAC is wholly lacking any factual allegations regarding any express or implied representations by Delta, or any conduct that would imply a mutual understanding regarding the protection of Plaintiff's personal and financial information. *See Armijo*, 854 Fed. App'x at 240 (finding no implied contract where "no factual allegations regarding formation or terms of the contract to be implied from the parties' conduct"). The fact that Delta received Plaintiff's information in the course of her employment does not show the required mutual assent necessary to support an implied contract. *See, e.g., Longenecker-Wells v. Benecard Servs. Inc*, 658 F. App'x 659, 662 (3d Cir. 2016) ("[Defendant] required Plaintiffs' personal information as a prerequisite to employment. This requirement alone did not create a contractual promise to safeguard that information, especially from third party hackers.")

Plaintiff also fails to point to any specific policies, manuals, or assurances that sufficiently support her claims that a contract for data protection exists. *See Morales v. Supreme Maint. Inc.*,

No. 21-cv-01044, 2022 WL 2290605, at *7 (D.N.M. June 24, 2022) (no implied contract of employment where "Plaintiff has failed to specifically allege what 'policies, practices, assurances, and other express and implied statements' were presented to her"); *see also Archey v. Osmose Utils. Servs.*, No. 20-cv-05247, 2022 WL 3543469, at *4 (N.D. Ill. Aug. 18, 2022) (noting that "many of the courts that have found an implied contract in the employee-employer data breach context have done so when the plaintiffs were able to point to some document, expression, or action of the employer which indicated an intention to protect the employee's personal information" and citing to cases supporting same). Consequently, such allegations are insufficient to establish an implied contract between Delta and Plaintiff.

Moreover, Plaintiff failed to adequately allege damages on her implied contract claim. "As a general rule, the amount of damages claimed for breach of contract must be reasonably ascertainable." *Unified Contractor, Inc. v. Albuquerque Hous. Auth.*, 2017-NMCA-060, ¶ 56, 400 P.3d 290. "Damages which are speculative, conjectural, or remote are not to be considered for compensation." *City of Santa Fe v. Komis*, 1992-NMSC-051, ¶ 11, 114 N.M. 659, 845 P.2d 753 (internal quotation marks and citation omitted). Plaintiff alleges that she suffered the "threat" of identity theft, actual identity theft, loss of the confidentiality of her data, illegal sale of the compromised data on the dark web, lost work time, and other economic and non-economic harm. FAC ¶ 109. As stated above, such allegations are wholly speculative.

C. Plaintiff's claim for unjust enrichment fails.

Under New Mexico law, a claim for unjust enrichment requires: "(1) another has been knowingly benefitted at one's expense (2) in a manner such that allowance of the other to retain the benefit would be unjust." *Ontiveros Insulation Co. v. Sanchez*, 2000-NMCA-051, ¶ 11, 129 N.M. 200, 3 P.3d 695.

Plaintiff alleges that Delta "received profits, benefits, and compensation" and Plaintiff did not receive the benefit of the bargain because she "paid for products/services that did not satisfy the purposes for which they bought/sought them." FAC ¶¶ 116-17. Plaintiff also alleges that Delta "failed to disclose facts pertaining to its substandard information systems" which apparently

"denied Representative Plaintiff and Class Members the ability to make a rational and informed purchasing decision and took undue advantage" of Plaintiff. *Id.* ¶ 115.

It is unclear exactly how the above allegations support an unjust enrichment claim, particularly as Delta employed Plaintiff and presumably paid her for such services (indeed, Plaintiff does not allege that Delta failed to compensate her). Plaintiff's conclusory allegations concerning "profits, benefits, and other compensation" by Delta is simply implausible, and Delta certainly has not been unjustly enriched by the security incident or retaining Plaintiff's personal information. *See Gordon v. Chipotle Mexican Grill, Inc.*, 344 F. Supp. 3d 1231, 1249 (D. Colo. 2018) (dismissing unjust enrichment claim following a data breach against Chipotle because plaintiffs "received the food services for which they paid" despite the security incident); *see also Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 50 (D. Ariz. 2021) (dismissing unjust enrichment claims because employee plaintiffs made only conclusory claims that defendant's data security was inadequate and thus there was no way to establish that defendant was enriched, or that employees were impoverished, through the exchange of labor).

Accordingly, Plaintiff's unjust enrichment claim also fails.

VI. Conclusion

Based on the foregoing, Delta respectfully requests the Court to dismiss Plaintiff's FAC in its entirety for lack of standing, or in the alternative, dismiss the FAC as each of her claims for negligence, breach of implied contract, and unjust enrichment fail to state a claim upon which relief may be granted, without leave to amend.

Respectfully submitted,

MODRALL SPERLING ROEHL HARRIS & SISK, P.A.

By: */s/ Kevin D. Pierce*

Jennifer G. Anderson
Kevin D. Pierce
Post Office Box 2168
Albuquerque, New Mexico 87103-2168
Telephone: (505) 848-1800
jga@modrall.com
kdp@modrall.com

AND

NORTON ROSE FULBRIGHT US LLP
Judith A. Archer
1301 Avenue of the Americas
New York, New York 10019-6022
Telephone: (212) 318-3446
judith.archer@nortonrosefulbright.com

Eva Yang
555 South Flower Street
Forty-First Floor
Los Angeles, California 90071
eva.yang@nortonrosefulbright.com

Attorneys for Defendant Delta Group Electronics

CERTIFICATE OF SERVICE

IT IS HEREBY CERTIFIED that on this 13th day of January, 2023, the foregoing was filed electronically through the CM/ECF system, causing all parties or counsel to be served by electronic means, as more fully reflected in the Notice of Electronic Filing.

MODRALL SPERLING ROEHL HARRIS & SISK, P.A.

By: */s/ Kevin D. Pierce*
Kevin D. Pierce

10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
VJY528SGAW

000117

Eveline Jean Mccombs
[redacted]

June 17, 2022

Dear Eveline Mccombs:

Delta Group Electronics, Inc. ("Delta Group") recognizes the importance of protecting the information we maintain. We are writing to notify you that we identified and addressed an incident that involved some of your personal information. This notice explains the incident, measures we have taken, and additional steps you may consider taking in response.

What Happened? On November 5, 2021, we learned of an incident involving unauthorized access to certain computer systems on Delta Group's network. Upon discovering the incident, we promptly took steps to secure our systems, began an investigation, and engaged a cybersecurity firm to assist. The investigation determined that an unauthorized actor accessed our systems and acquired a limited number of files from certain servers between November 2, 2021 and November 5, 2021.

What Information Was Involved? On April 1, 2022, we completed a thorough review of the files acquired by the unauthorized actor and determined that the files contained your name and Social Security number, driver's license number, and financial account number ending in [redacted], [redacted] and [redacted].

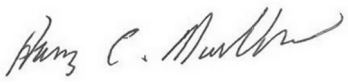
What We Are Doing. We wanted to let you know this happened and assure you we take it very seriously. To help prevent a similar incident from occurring in the future, Delta Group has implemented additional security measures to enhance the security of our network and re-educated our employees concerning data security. We are also offering you a free credit and identity monitoring services through IDX. IDX identity protection services include one year of triple bureau credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

What You Can Do. We encourage you to remain vigilant by regularly reviewing your credit reports and financial account statements for any unauthorized activity. If you see charges or activity that you did not authorize, please contact the relevant provider immediately. You may also contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and use the Enrollment Code provided above. Please note the deadline to enroll is **September 17, 2022**.

EXHIBIT A

For More Information. For more information on identity theft prevention, as well as some additional steps you can take to protect your information, please see the pages that follow this letter. Should you have any further questions or concerns regarding this incident, please contact our dedicated help line at 1-800-939-4170, Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,



Harry Mueller
President & CEO
Delta Group Electronics, Inc.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to review your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Delta Group Electronics, Inc. is located at 4521 Osuna Rd NE, Albuquerque, NM 87109, and can be reached by telephone at (888) 389-8415.

The Additional information for residents of the following states:

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.